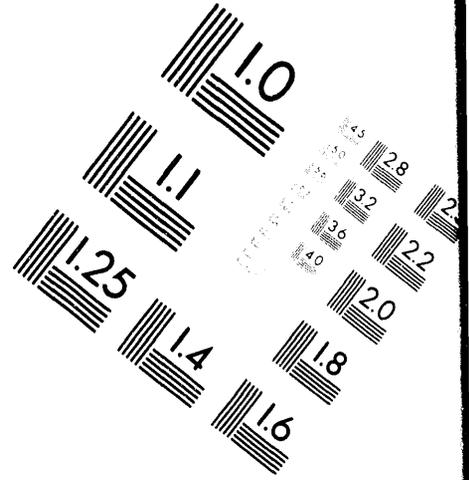
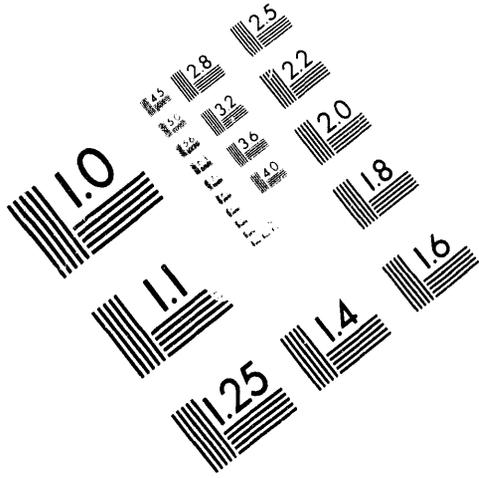




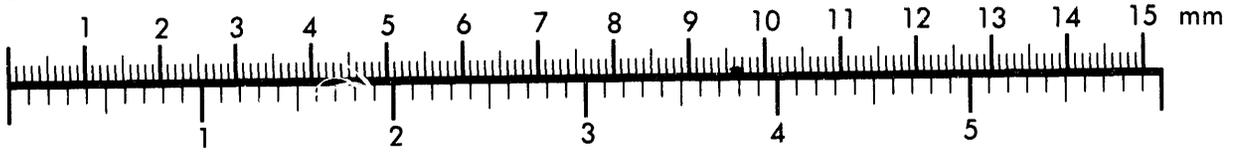
AIM

Association for Information and Image Management

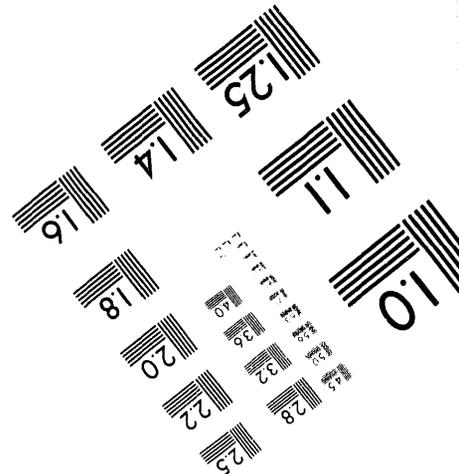
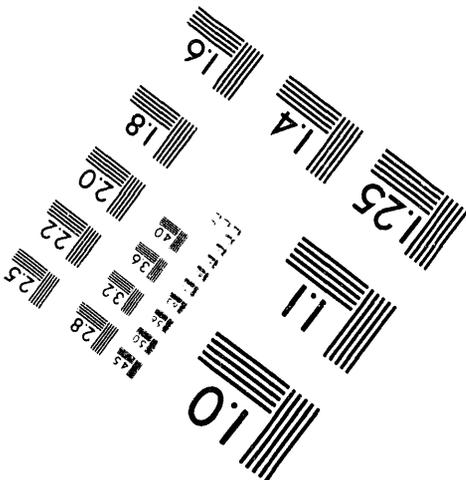
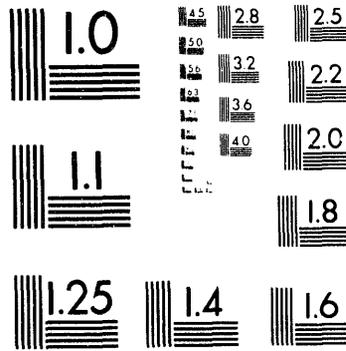
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910
301/587-8202



Centimeter



Inches



MANUFACTURED TO AIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 1

DOE DISS/ET PILOT SYSTEM

R. Scott Strain

Lawrence Livermore National Laboratory
Livermore, CA

Ernest E. Wagner

U.S. Department of Energy
Washington, D.C.

ABSTRACT

The U.S. Department of Energy (DOE) Office of Safeguards and Security initiated the DOE Integrated Security System / Electronic Transfer (DISS/ET) for the purpose of reducing the time required to process security clearance requests. DISS/ET will be an integrated system using electronic commerce technologies for the collection and processing of personnel security clearance data, and its transfer between DOE local security clearance offices, DOE Operations Offices, and the Office of Personnel Management. The system will use electronic forms to collect clearance applicant data. The forms data will be combined with electronic fingerprint images and packaged in a secure encrypted electronic mail envelope for transmission across the Internet. Information provided by the applicant will be authenticated using digital signatures. All processing will be done electronically.

INTRODUCTION

The U.S. Department of Energy (DOE) personnel security activities (like those of any government agency or department) involve the processing and filing of large amounts of paper materials. Security forms and investigative reports are manually prepared and must be manually maintained in files. Consequently, the transmission of information (investigative reports, files between offices, etc.) is slow and resource intensive. In order to speed the security clearance process, the DOE Office of Safeguards and Security (OSS) has begun a joint project with the U.S. Office of Personnel Management (OPM) to redesign the security clearance process. The project is

the Electronic Transfer module of the DOE Integrated Security System (DISS/ET).¹

In order to effectively use existing technology to reduce security clearance processing time and the amount of paper involved in the personnel security process, program activities and procedures are themselves being redesigned. The re-design is being focused on the electronic transfer and processing of data, as opposed to merely producing paper products more quickly. The re-design encompasses both internal (to the department) and external activities. These activities include, for example, establishing (at the 12 departmental offices that have program responsibilities) the capability to: electronically send requests for investigations to OPM; electronically receive completed investigations from OPM; generate and maintain electronically personnel security files; directly add data to and delete data from the personnel security files; permit personnel security specialists to access the file data base via a personal computer at their work location; and transfer to and receive from other DOE offices the contents of an entire personnel security file.¹

IMPLEMENTATION OVERVIEW

The project to develop the DISS/ET integrated and automated system was begun in July 1993. The overall project will consist of three phases. The first phase, now completed, provided the requirements definition. The second phase is automating the front-end of the clearance process, including data collection and transfer to OPM. The third phase will automate the work-flow of the back-end of the clearance process, including transfer of the

MASTER

EP

DOE DOCUMENTATION CENTER

investigation results from OPM to DOE and the documentation of the clearance decision.

The second phase of the project is developing the computer systems and procedures required to automate the security clearance work-flow for the data collection and electronic transfer of information to OPM. It will result in the computerization of the Questionnaire for Sensitive Positions (QSP). The system will pass the information electronically to OPM using trusted electronic mail systems. An information management system will be developed for: maintaining data files, monitoring the status of cases, and providing for data integrity and privacy. All data received in electronic form will be automatically stored in a database.

An important step in the second phase of the DISS/ET project will be a pilot system linking one DOE contractor (Lawrence Livermore National Laboratory), one DOE field office (DOE Oakland Operations Office), and OPM. Once the pilot system has been fully tested, the decision to extend the system throughout the DOE will be made. The extension of the pilot system to a full production system throughout the DOE Complex will require a considerable investment in equipment and in the development of both computer systems and management infrastructure. This investment will be made only after the pilot system is operational and evaluated.

The back-end of the clearance process will be automated in the third phase of the DISS/ET project. In this phase, the project will implement trusted electronic mail for the transfer of the results of the OPM investigations to the DOE field offices. Activities to be automated at the DOE field offices include documentation and assistance of the clearance-granting process. This will include the computer capability to easily query the information management system and review all information pertinent to a case. The system will perform any desired data manipulations and will present information in the proper form for documenting the clearance decision. Additional enhancements to the second phase systems may also be made as part of this phase.

CLEARANCE APPLICANT INTERFACE

Once individuals are notified that they need to begin the process for a security clearance, they will be asked to schedule an appointment with their local security office, much like the paper process works today. At the security office, they will be fingerprinted (by a livescan, ink, or inkless process). They will also be given a private key (on a floppy disk) for use as a digital signature. The private key will be protected by a password that the applicant chooses (and, of course, by the applicant's physical protection of the disk). The applicant will also be asked to sign at least one authorization form. After the applicant leaves the security office, the applicants fingerprints and the signed paper forms will be electronically scanned, encrypted, and forwarded to the cognizant DOE field office. A multi-part electronic mail message will package the electronic fingerprint card, the signed authorization form, and other necessary data.

The applicants will return to the desktop computer in their office (or one in their secretary's office, or one set aside in the local security office). Both Macintosh and MS Windows computers will be supported. From this desk top computer the applicant will be able to retrieve from a computer in the DOE field office or other server, the software for completing the QSP (currently Form SF86). This form will be programmed in a commercial software package and will be user friendly for users that do not normally use computers. The applicant will enter the required data directly into the computer. The software will perform checks for: accuracy (e.g., zip codes), internal consistency (e.g., between time periods), and completeness. For reinvestigations when earlier forms data are on electronic file, the appropriate information will be provided automatically for editing by the applicant to minimize the data that the applicant needs to enter for the reinvestigation. Once the form is completed, the software will encrypt the form and prompt the applicant to digitally sign the form using his/her private key, which is resident on the floppy disk he/she was given in the security office. The

encrypted and digitally signed information will then be forwarded to the cognizant DOE operations office.

SYSTEM ARCHITECTURE

The DISS/ET system will consist of 12 regional personnel security databases (RPS), one at each DOE field office. These databases will be linked with each other and the OPM over the Internet. The RPS will reside on a

UNIX workstation. The OPM mainframe computer, which handles the Personnel Investigations Processing System (PIPS) database, will be connected to a gateway UNIX workstation. These computers will all communicate using electronic mail protocols. The architecture for one RPS is shown in Fig. 1. There may be multiple applicant user computers, clearance office users, and DOE field office users. Only one of each is shown in Fig. 1.

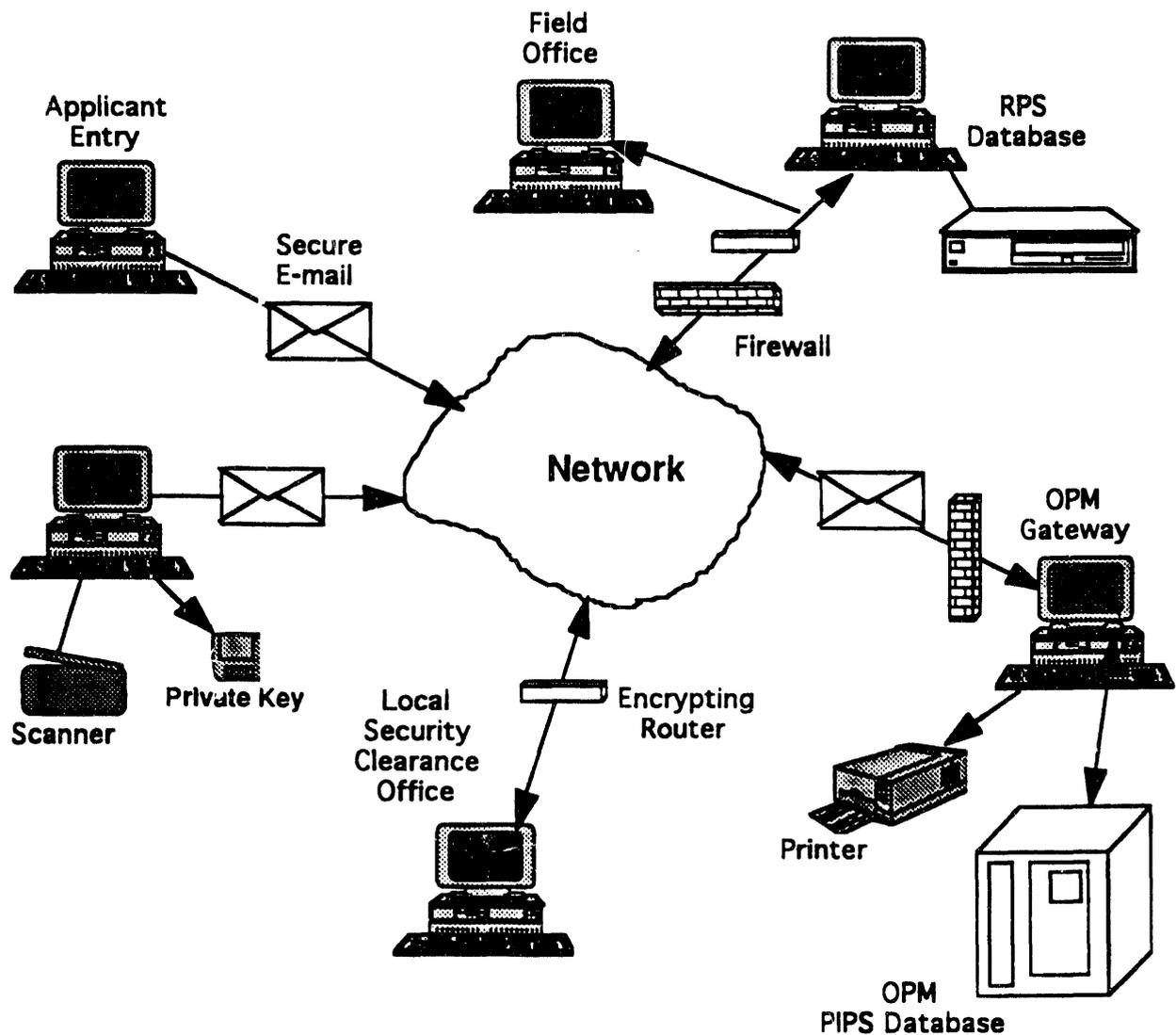


Figure 1. Schematic of DISS/ET system architecture.

The local security clearance office will be able to access the RPS in order to set up a "folder" for new applicants and their information, review selected portions of the applicant's forms data, track clearance status, include a clearance request justification, review the applicant's file for completeness, and flag the applicant's file for review by DOE once it is complete. Because, the local security clearance office access to the RPS needs to be in real time in order to be efficient, the link between the local security clearance office and the RPS will not use e-mail, but will use encrypting routers for security.

After a file has been initiated by the local security clearance office and has been flagged by that office as being complete, the DOE field office will be alerted to initiate a security clearance case. They will review and edit the data as necessary and then send the case on to OPM for the investigation. The DOE field office will be able to monitor and track all cases. All clearance data will be maintained electronically on the RPS. In the third phase of DISS/ET the OPM will send the investigation results to the DOE field office electronically and the clearance will be adjudicated using all electronic data.

DATA SECURITY AND INTEGRITY

Much of the data on the RPS is unclassified sensitive information and must be protected according to DOE Order 1360.2B and the Privacy Act of 1974. There are several security issues: controlled access to data on the RPS; intruder attacks on the RPS and the OPM gateway; electronic remains on interface computers; and data transmission.

The RPS computer itself will be in a physically secure location. All of the data on the RPS will be maintained in a commercial-off-the-shelf relational database management system (RDBMS). All access to the data will be through the RDBMS software. The RDBMS software will allow for controlled access for viewing, updating, and deleting data. It will also provide an audit trail of all data access. This access will be controlled by user privilege. A user's privilege will be determined by the software based on the user login with the user's account and password.

User privilege will be controlled by a responsible individual in the DOE field office. Each attempt to access the DISS/ET database on the RPS will result in an audit trail, including unauthorized requests, read requests, and updates to data or status. The audit entry will include the user identification, data and time, data accessed, and actions taken.

The DISS/ET RPS and the OPM gateway will be connected to the Internet and therefore must be well-protected against attacks by intruders. All of these computers will be protected by "firewalls." The DISS/ET firewalls will consist of both screening routers and a bastion host computer. Firewalling involves disabling capabilities that an intruder may use to penetrate the systems and using secure versions of those capabilities necessary for system functionality. For the OPM gateway, all network services except e-mail will be disabled. E-mail will be further restricted to receipt of messages from DISS/ET RPS and in the expected privacy enhanced mail format. The RPS firewalls will be similar, except they will allow non-e-mail access through encrypting routers from the local security clearance offices.

Any electronic remains on applicant user entry computers (which will not be subject to the same use and physical security constraints as the local security clearance office and DOE field office computers) will be purged at the termination of each applicant user session. This purge will include any DISS/ET data on the display screen, the hard disk, and the computer's internal memory.

All data transmission, except that done through encrypting routers, will be done using secure e-mail messages. The systems will use the Internet standards of Simple Mail Transport Protocol (SMTP), Privacy Enhanced Mail (PEM), and Multipurpose Internet Mail Extensions (MIME). These protocols provide not only privacy—only the intended recipient can read the message—but also authentication of both the sender and the message. The security is provided by DES encryption and the authentication is provided by digital signatures using public key

cryptography. (Public key cryptography is also used for the DES key exchange.)

PILOT SYSTEM STATUS

The pilot system is scheduled to be operational in September of this year. At that time most of the second phase functionality will be in place. Lawrence Livermore National Laboratory (LLNL) clearance applicants will be able to use a computer in the local security clearance office to enter their personnel security forms data. Most forms will be automated, including entry, validation and printing. Applicants' signed forms and fingerprints will be scanned sent to the RPS in the DOE Oakland Operations Office. Most of the contractor and DOE user interfaces will be available in September. The DOE Oakland Operations Office will send the clearance data to the OPM over the Internet. As noted earlier, the ability of OPM to send investigation results to the DOE Oakland Operations Office will not be available until the third phase.

The pilot system is expected to be operated in parallel with the existing paper system for several months. Based on that operational experience, changes and improvements to DISS/ET will be made and tested. The system will then be implemented across the DOE complex in stages during the 1995 calendar year.

ACKNOWLEDGMENT

Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

REFERENCES

1. *A More Responsive, Practical, and Efficient Personnel Security Program for the Department of Energy, A Report to the Director, Office of Intelligence and National Security*, by the Personnel Security Program Review Task Force, U.S. Department of Energy, Washington, D.C., January 1994.

DATE

FILMED

11/9/94

END

